PATENT APPLICATION
Docket No.: 15964.5.1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	David L. Summers	) Art Unit) 2131
Serial No.:	09/767,465	)
Confirmation No.:	2143	)
Filed:	January 22, 2001	)
For:	SPONTANEOUS VIRTUAL PRIVATE NETWORK BETWEEN PORTABLE DEVICE AND ENTERPRISE NETWORK	)
Examiner:	Dohm Chankong	)
Customer No.:	022913	)
Appeal No.:	_______________	)

Commissioner for Patents
PO Box 1450
Alexandria, Virginia 22313-1450

BRIEF OF APPELLANTS

This is an appeal from the Final Office Action dated August 30, 2005 wherein the Examiner rejected Claims 1-45. This Brief is being filed under the provisions of 35 U.S.C. § 134 and 37 C.F.R. § 41.37. This Brief is accompanied by the requisite fee of $500 as set forth in 37 C.F.R. § 41.20(b) The Commissioner is hereby authorized to charge any additional fees associated with this communication, or to credit any overpayment, to Deposit Account No. 23-3178.

TABLE OF CONTENTS

LIST OF REFERENCES

U.S. Patent Documents

U.S. Patent No. 6,563,800 to *Salo* et. al.
U.S. Patent No. 6,411,986 to *Susai* et. al.
U.S. Patent No. 6,765,881 to *Rajakarunanayke*
U.S. Patent No. 6,292,905 to *Wallach* et.al.
U.S. Patent No. 6,138,049 to *McLaughlin*
U.S. Patent No. 6,081,900 to *Subramaniam*
U.S. Patent No. 6,295,551 to *Roberts* et. al.
U.S. Patent No. 6,631,416 to *Bendinelli* et. al.
U.S. Patent No. 6,529,500 to *Pandharipande*
U.S. Patent No. 6,032,227 to *Shaheen*

I. REAL PARTY IN INTEREST

The real party in interest is Intellisync Corporation, the assignee of record.

II. RELATED APPEALS AND INTERFERENCES

None.

III. STATUS OF CLAIMS

Claims 1-45 are pending in this application and claims 46-48 have been cancelled. Claims 1-45 were rejected in the Final Office Action dated August 30, 2005.

IV. STATUS OF AMENDMENTS

The Appellant did not submit any amendments subsequent to the Final Rejection mailed August 30, 2005.

V. SUMMARY OF INVENTION

Embodiments of the present invention provide a method for enabling a user to access network data of a remote enterprise network through a data tunnel established between a data center and the remote enterprise network. The data tunnel operates as a virtual private network. A remote user, with respect to the enterprise network, is enabled to access network data stored at the enterprise network by communicating with a data center that has an established data tunnel with the enterprise network. (Page 7, lines 12-14.) Users are able to access network data through a secure data tunnel through a pre-opened Internet port. (Page 7, lines 2-7.) A secure data tunnel that is pre-opened between the data center and the enterprise network eliminates the need to install the additional software or hardware at the business firewall and enables the user to access the network data without opening additional ports or holes in the firewall of the enterprise network. *(Id.)*

According to one embodiment and with reference to Figures 3 and 4, a data center 44 receives a data request 50 from a remote enterprise network 40 and establishes a data tunnel 42 with the data center 44 by transmitting reply data 53 to the enterprise network 40. (Page 14, line 23 through page 15, line 2.) The data center 44 continues to transmit reply data 53 in an ongoing manner such that the data tunnel 42 is kept open between the data center 44 and the enterprise network 40. (Page 16, lines 2-3.) Next, the data center 44 receives an access request 70 for network data 22 (stored at the enterprise network 40) from a user 10. (Page 17, lines 1-2.) The data center 44 (using a web server 60) transmits the access request 70 to the enterprise network 40 over the already open data channel 42. (Page 20, lines 9-12; Page 17, line 22 through Page 18, line 2.) The data center 44 then receives the requested network data 22 from the enterprise network 40. (Page 21, lines 3-4.) Finally, the data center 44 transmits the network data 22 to the user 10. (Page 21, lines 12-13.)

In another embodiment and with reference to Figure 2, after establishing a data tunnel between the enterprise network and the data center such that the data tunnel is kept open as the data center continues to transmit reply data as described above, the data center 44 receives network data 22 over the data channel 42. (Page 25, line 9-10.) This network data 22 is cached at a database 62 of the data center 44. (Page 25, line 10). The data center 44 next retrieves the cached network data from the database 62 in response to an access request 70 from the user 10 and then transmit the cached network data to the user 10. (Page 26, 6-8).

Embodiments of the invention thus enable a user to access network data behind a firewall using a pre-opened data channel between a data center and the enterprise network without requiring the user to obtain access using predefined, and discrete VPN node locations that must be configured with VPN software and hardware. The pre-opened and kept open data channel enables the user to access network data without requiring another port or hole in the firewall as would be required by a separate VPN . (Page 7, lines 5-7, 8-11, and 14-18.)

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Issue 1: Whether claims 1-45 are indefinite under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention in view of the limitation "without requiring a virtual private network node to be placed at the firewall".

Issue 2: Whether claims 1, 13, 23, 28, and 34 are unpatentable under 35 U.S.C. § 103(a), over U.S. Patent No. 6,563,800 (*Salo*) in view of U.S. Patent No. 6,411,986 (*Susai*) in further view of U.S. Patent No. 6,765,881 (*Rajakarunanayke*).

Issue 3: Whether claims 39-45 are unpatentable under 35 U.S.C. § 103(a) over *Salo*, *Susai*, and *Rajakarunanayke* in further view of U.S. Patent No. 6,032,227 (*Shaheen*).

Issue 4: Whether claims 3-7 are unpatentable under 35 U.S.C. § 103(a) over *Salo, Susai,* and *Rajakarunanayke* in further view of U.S. Patent No. 6,292,905 (*Wallach*).

Issue 5: Whether claims 8, and 11-12 are unpatentable under 35 U.S.C. § 103(a) over *Salo, Susai, Rajakarunanayke,* and *Wallach* in further view of U.S. Patent No. 6,138,049 (*McLaughlin*).

Issue 6: Whether claims 17, 18 and 25 are unpatentable under 35 U.S.C. § 103(a) over *Salo, Susai,* and *Rajakarunanayke* in further view of U.S. Patent No. 6,081,900 (*Subramaniam*).

Issue 7: Whether claim 19 is unpatentable under 35 U.S.C. § 103(a) over *Salo, Susai,* and *Rajakarunanayke* in further view of U.S. Patent No. 6,295,551 (*Roberts*).

Issue 8: Whether claims 20 and 24 are unpatentable under 35 U.S.C. § 103(a) over *Salo, Susai,* and *Rajakarunanayke* in further view of U.S. Patent No. 6,631,416 (*Bendinelli*).

Issue 9: Whether claim 36 is unpatentable under 35 U.S.C. § 103(a) over *Salo, Susai,* and *Rajakarunanayke* in further view of U.S. Patent No. 6,529,500 (*Pandharipande*).

VII. GROUPING OF CLAIMS

Claims 1-38 stand or fall together and claim 1 is considered representative of the group.

Claims 39-45 stand or fall together and claim 39 is considered representative of the group.

VIII. ARGUMENTS

Issue 1: Whether claims 1-45 are indefinite under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention in view of the limitation "without requiring a virtual private network node to be placed at the firewall".

On page 3 of the Final Office Action, the Examiner states:

> Claims 1, 13, 23, 28, 24, and 39 are rejected because of the limitation "without requiring a virtual private network node to be placed at the firewall". It is unclear from the claim language what is meant by "placed at the firewall" and does not distinctly claim where a node can or cannot be placed.

The essential inquiry pertaining to the requirements of § 112, second paragraph, is whether the claims set out and circumscribe a particular subject matter with a reasonable degree of clarity and particularity. *See* MPEP § 2173.02. Definiteness of claim language must be analyzed, not in a vacuum, but in light of:

(A) The content of the particular application disclosure;
(B) The teachings of the prior art; and
(C) The claim interpretation that would be given by one possessing the ordinary level of skill in the pertinent art at the time the invention was made. *See Id.*

The Board of Patent Appeals and Interferences has further stated that:

> In rejecting a claim under the second paragraph of 35 U.S.C. § 112, it is incumbent on the examiner to establish that one of ordinary skill in the pertinent art, when reading the claims <u>in light of the supporting specification</u>, would not have been able to ascertain with a reasonable degree of precision and particularity the particular area set out and circumscribed by the claims. *See Ex parte* Wu, 10 USPQ2d 2031,2033 (B.P.A.I. 1989) (*emphasis added*). .

The Examiner makes no reference in the Office Action, as required above, to the content of Applicants disclosure relating to the interpretation of the language "placed at the firewall" and instead relies on specific implementations disclosed in *Salo*. Further, it is not the normal function of a claim to disclose the invention, but to point out the features of novelty in the invention as disclosed in the specification. *See* Bocciarelli v. Huffman, 232 F.2d 647, 109 USPQ 385, 388 (C.C.P.A. 1956).

In this case, the discussion provided by the Examiner only references *Salo* and does not consider the content of the present disclosure. Further, by focusing on a few words without considering Applicants' disclosure or without considering each claim as a whole, the Examiner is interpreting the rejected language in a vacuum.

One of the arguments presented by the Examiner is that *Salo* discloses, in figure 5a, that -- the server and firewall are two distinct entities and it can be argued that since they are distinct devices, they are separate from one another – then the server is not "placed at the firewall". *See* Final Office Action Page 3. The Examiner further argues that "in figure 5b, *Salo* seems to have utilized the Ipsec router as a firewall and so it can be argued that the firewall and the router are the same device and then therefore, the router is not 'placed at the firewall'". *See* Office Action Page 3.

As illustrated below, a specific implementation of a VPN (as illustrated in *Salo*) and/or a firewall does not render the language rejected by the Examiner indefinite. The arguments of the Examiner, for example, fail to take into account the content of the Applicants' disclosure as well as the teachings of the cited art. Both *Salo* and the present disclosure use the terms firewall and virtual private network in a consistent manner.

For example, *Salo* teaches that an enterprise may "install a firewall (or firewalls) to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own subscribers have access to." *See Salo* col. 8, lines 35-38. Applicants' disclosure similarly states that "a firewall is a security mechanism that prohibits access through designated ports of a network and ensures network data cannot be accessed from an unauthorized user from outside of the firewall." *See* Page 15, lines 10-13. The description of a firewall in both *Salo* and of the present disclosure are similar: Both *Salo* and the present disclosure suggest that a firewall is a security mechanism to ensure that network data is protected.

With regard to virtual private networks (VPNs), *Salo* suggests that by encrypting all data transmitted over a network 402, the data center 190 and the enterprise server 403 communicate with one another as if they were on a private network. *See* col, 12, lines 38-41. *Salo* then generally teaches that "this type of encrypted network communication is called a virtual private network." *See* col. 12, lines 42-43. Figures 5A and 5B serve to illustrate specific embodiments of the implementation of a VPN between the data center 190 and the enterprise network 403. *See* col. 12, lines 44-46.

Finally, *Salo* indicates that the firewall 520 may be optionally implemented in conjunction with the VPN server 515. *See* col. 12, lines 56-57. As a result, *Salo* teaches that the VPN establishes an encrypted network connection and that the firewall can still be used to limit unauthorized outsiders from accessing the private data resources of the enterprise network 403. *See* col. 12, lines 42-43, 56-59. Thus, *Salo* considers embodiments of a VPN being implemented with a firewall.

The present disclosure is also abundantly clear on what constitutes a VPN as well as what constitutes a VPN node placed at a firewall. The disclosure states, for example, that it is possible for a "remote business 23 to communicate with the business network 12 through a VPN tunnel 24, as shown between VPN node 16 and VPN node 26." *See* Page 3, lines 13-15. Figure 1 further illustrates a VPN node 16 placed at the firewall 20. Thus, the content of the present disclosure provides ample support for the terms VPN node, firewall and an example of a VPN node placed at the firewall. *See* Figure 1. *Salo*, as described above, also considers that a firewall can work in conjunction with a VPN server. *See* col. 12, lined 56-57.

The Federal Circuit has held that "if the meaning of the claim is discernible, even though the task may be formidable and the conclusion may be one over which reasonable persons will disagree, we have held the claim sufficiently clear to avoid invalidity on indefiniteness grounds." *Exxon Research & Eng'g Co. v. United States*, 265 F.3d 1371, 1375, 60 USPQ2d 1272 (Fed. Cir. 2001).

Rejecting the language "placed at the firewall" reads the language in a vacuum. The claims require "without requiring a virtual private network node to be placed at the firewall" while the Examiner rejects the language "placed at the firewall". The failure of the Examiner to read the claim as a whole suggests that the language is being read in a vacuum, which is not allowed.

Further, "there is nothing inherently ambiguous or uncertain about a negative limitation." *See* MPEP § 2173.05(i). While the Examiner indicates that the claim language "does not distinctly claim where a node can or cannot be placed" (*see* Office Action Page 4), there is no corresponding requirement in the claims of either placing or not placing the VPN node. Rather, the claim requires "the data tunnel operating as a virtual private network through a firewall of the remote enterprise network without requiring a virtual private network node to be placed at the firewall." Read as a whole, the claim language excludes "requiring a virtual private network node to be placed at the firewall".

For at least these reasons, the exact language rejected by the Examiner of "placed at the firewall", considered in light of the present disclosure and in view of the cited art as discussed above, circumscribes a particular subject matter with a <u>reasonable</u> degree of clarity and particularity. As previously stated, it is not the normal function of a claim to disclose the invention. *See* Bocciarelli v. Huffman, 232 F.2d 647, 109 USPQ 385, 388 (C.C.P.A. 1956).

Appellant respectfully requests that the rejection of claims 1-45 under 35 U.S.C. § 112, second paragraph, be overturned.

Issue 2: Whether claims 1, 2, 9, 10, 13-16, 21-23, 26-35, 37, and 38 are unpatentable under 35 U.S.C. § 103(a), over U.S. Patent No. 6,563,800 (*Salo*) in view of U.S. Patent No. 6,411,986 (*Susai*) in further view of U.S. Patent No. 6,765,881 (*Rajakarunanayke*).

To set forth a *prima facie* case of obviousness the following elements must be shown, according to M.P.E.P. § 2143:

> (1) suggestion or motivation, either in the references themselves or in the knowledge available to one skilled in the art, to modify the reference or combine reference teachings;
>
> (2) a reasonable expectation of success; and
>
> (3) the combined references must teach or suggest all the claim limitations of the Appellant's claims.

The mere fact that the references can be combined is not sufficient to establish *prima facie* obviousness unless the prior art, in addition, suggests the desirability of the combination. *See* M.P.E.P. §2143.01.

The Examiner admits that *Salo* does not disclose "establishing the data tunnel in response to receiving a data request from the remote enterprise network, continuing to transmit reply data to the remote enterprise network in an ongoing manner such that the data tunnel is kept open, or that the access request is transmitted using an existing data tunnel that has been established and exists prior to the data center having received the access request." *See* Page 5 of Office Action.

The Examiner attempts to remedy this deficiency by citing *Susai* as disclosing "transmitting an access request to a remote network (his collection of servers) using an existing data connection that has been established (between the interface device and the server) and exists prior to the interface device having received the access request . . . and continuing to transmit the reply data to the remote network in an ongoing manner such that the data tunnel is kept open." *See* Page 6 of Office Action.

Applicants disagree and submit that *Susai* does not teach these elements. Applicants agree that *Susai* is related to Internet client-server applications and to multiplexing connections between clients and servers over the Internet. *See* col. 2, lines 49-51. However, *Susai* does not teach or suggest maintaining an data channel between a data center and a remote enterprise network as suggested by the Examiner. Rather, the connection of *Susai* that is not closed is between an interface unit and a server and not between a client and a server. *See* col. 2, lines 55-63 (*emphasis added*).

In the claims, a data tunnel is established between the data center and the remove enterprise network by first receiving a data request from the remote enterprise network. The data tunnel is further established through a firewall of the remote enterprise network. In contrast, the invention of *Susai* is "implemented within an interface unit connecting a plurality of servers to the Internet, which is in turn connected to a plurality of clients." *See* col. 2, lines 51-54.

The interface unit of *Susai* is "an intelligent network interface card with a CPU inside a server . . . [and] can also be a load balancer, bandwidth manager, firewall, router, switch, computer system, or any other network device that is located between a client and server." *See* col. 3, lines 62-67. Figure 2 of *Susai* illustrates that all Internet traffic with the server farm passes through the interface unit 202. *See* col. 4, lines 4-6. As described above, it is a connection between the interface unit and one of the servers that is kept open. Even if the interface unit functions as a firewall, it is a firewall between the clients and the servers, whereas the connection taught by *Susai* is between the interface unit and the servers. Therefore, the open connection of *Susai* is not <u>through</u> a firewall as required by the claims. Rather, the open connection of *Susai* would be behind the firewall of the servers because the interface unit would function as the firewall. Therefore, the open connection of *Susai* between the interface unit and the servers is not a virtual private network as required by the claims.

In addition, *Susai* teaches that achieving a connection between a client and a server includes two separate connections. The first is between the client and the interface unit. *See* col. 2, lines 55-57. The second connection is between the interface unit and the server. *See* col. 2, lines 57-58. Finally, *Susai* specifically teaches that the connection between the client and the user interface is <u>closed</u>. *See* col. 2, lines 60-61. The teaching of explicitly closing the connection between the client and the user interface effectively closes the connection between the client and the servers. *Susai* therefore teaches away from the pending claims, which require the data channel be kept <u>open</u> between the data center and the remote enterprise network.

The teachings of *Susai* do not, therefore, remedy the deficiencies of *Salo*. Claim 1, for example, requires that the data tunnel operate as a virtual private network through the firewall of the remote enterprise network. The data tunnel between the data center and the remote enterprise is akin to the connection between the client and the interface unit, not the connection between the interface unit and the server because the unit interface taught by *Susai* is integrated with the servers and is accessible to clients over the Internet. *See* col. 3, lines 62-67. In fact, *Susai* clearly suggests that the unit interface is part of the server network. *See* col. 3, lines 60-61 (interface unit is a card with a CPU <u>inside</u> a server.)

The teaching of multiplexing a connection between an interface unit and multiple servers in *Susai* does not teach that the connection between the unit interface and the server is a virtual private network. In fact, *Susai* has the goal of reducing loading problems by keeping a connection with one of the servers open. Requiring the interface unit to establish virtual private networks with the servers would tend to increase the overhead that *Susai* wants to avoid by reducing connection loading.

Further, there is no suggestion or teaching in *Susai* that the connection opened between the interface unit and the sever is through a firewall, as required by the claims. As previously stated, even where the interface unit functions as a firewall, the open connection is not through the firewall as required by the claims. Rather, the interface unit is an end point of the open connection between the interface unit and a server.

Also, *Susai* teaches that it is the interface unit that opens the connection with the server. *See* col. 4, lines 34-35. The data center the claims, in contrast, first receives a data request from the remote enterprise network. The data center then keeps the data channel open by continuing to transmit reply data in an ongoing basis. This is admitted by the Examiner in the statement that "*Salo* and *Susai* do not explicitly disclose that the tunnel is established in response to receiving a data request from the remote enterprise network, establishing the data tunnel with the remote enterprise network, by transmitting reply data to the remote enterprise network." *See* Office Action Page 6. Thus, *Susai* fails to teach the elements of the claims as alleged by the Examiner and therefore does not remedy the deficiencies of *Salo* admitted by the Examiner.

Rajakarunanayake is cited as disclosing the establishment of data tunnels between a corporate network and clients, but fails to teach or suggest the all of the limitations discussed above with respect to *Salo* and *Susai*.

Because all of the required elements of the claims are not taught by the combination of *Salo, Susai,* and *Rajakarunanayake,* a *prima facie* case of obviousness is not established. Further, because the connection taught by *Susai* is on the server side of the Internet relative to the clients, as shown in Figure 2 server, and because *Susai* teaches that the connection between the client and the unit interface is closed, there is no expectation of success in the combination of *Salo, Susai,* and *Rajakarunanayake.* In other words, the requirement of establishing a data tunnel through a firewall of the remote enterprise network without requiring a virtual private network node to be placed at the firewall, cannot be achieved as suggested by the Examiner.

Accordingly, the rejection of claims 1, 2, 9, 10, 13-16, 21-23, 26-35, 37, and 38 under 35 U.S.C. § 103(a) should be overturned.

Issue 3: Whether claims 39-45 are unpatentable under 35 U.S.C. § 103(a) over *Salo, Susai,* and *Rajakarunanayke* in further view of U.S. Patent No. 6,032,227 (*Shaheen*).

Claim 39 requires:

> establishing the data tunnel with the remote enterprise network by transmitting reply data to the remote enterprise network in response to receiving a data request from the remote enterprise network;
> continuing to transmit the reply data to the remote enterprise network in an ongoing manner to keep the data tunnel open;
> receiving network data from the remote enterprise network through the data tunnel, the data tunnel operating as a virtual private network through a firewall of the enterprise network without requiring a virtual private network node to be placed at the firewall . . . .

As discussed above regarding Issue 2, neither *Salo, Susai* and *Rajakarunanayke* fail to teach or suggest, alone or in combination, these requirements of claims 39-45. The data tunnel required by these claims is kept open and is required to be through a firewall of the enterprise network. The connection taught by *Susai,* is on the server side of the system between an interface unit and multiple servers and does not pass through a firewall. Further, *Susai* requires closing the connection with the client, whereas these claims require keeping the data tunnel between the data center and the enterprise network open by continuing to transmit reply data in an ongoing manner.

The Examiner cites *Shaheen* as teaching "a method of caching a copy of the network data in a database of the data center. Page 20 of Office Action. *Shaheen* is generally directed a mobile cache management system and teaches, for example, a cache management system that implements a replacement policy that preserves files with updates and a method that presents options to the system user to allow interactive cache management in response to cache limit detection. *See* col. 3, lines 40-47.

Cache management, however, does not teach or suggest receiving network data from the remote enterprise over a data channel that operates as a virtual private network through a firewall of the enterprise network and then caching the copy of the network data received over the data channel. Viewed as a whole, *Salo, Susai, Rajakarunanayke,* and *Shaheen* do not teach or suggest the pending claims.

Accordingly, the rejection of claims 39-45 under 35 U.S.C. § 103(a) should be overturned.

Issue 4: Whether claims 3-7 are unpatentable under 35 U.S.C. § 103(a) over *Salo, Susai,* and *Rajakarunanayke* in further view of U.S. Patent No. 6,292,905 (*Wallach*).

By virtue of their dependence on claim 1, claims 3-7 incorporate the limitations of claim 1. For reasons previously discussed, these elements are not taught or suggested alone or in combination over *Salo, Susai,* and *Rajakarunanayke. Wallach* was cited by the Examiner as teaching a method wherein a database of the remote enterprise network is notified which of the multiple servers is the designated server, the designated server notifying the database when the data tunnel is established. However, *Wallach* fails to teach or suggest, as required by claim 1:

> in response to receiving a data request from the remote enterprise network, establishing the data tunnel with the remote enterprise network by transmitting reply data to the remote enterprise network, the data tunnel operating as a virtual private network through a firewall of the remote enterprise network without requiring a virtual private network node to be placed at the firewall;
>
> continuing to transmit the reply data to the remote enterprise network in an ongoing manner such that the data tunnel is kept open . . . .

Wallach, in contrast to these requirements, teaches a fault tolerant access to a network resource, without hardware mirroring and involves an enhanced replicated network directory database that operates in conjunction with server resident processes to remap network resources in the event of a server failure. *See* col. 3, lines 39-42.

The rejection of claims 3-7 is further improper as one of skill in the art would not be motivated to combine these references when the claims are considered as a whole. Establishing a data tunnel between a data center and a remote enterprise network that is kept open by sending ongoing reply data is not suggested by processes to remap network resources in the event of a server failure. The Examiner is required to examine the claim as a whole rather than examine the elements in piecemeal fashion.

A review of the Office Action reveals that the Examiner has included separate references to represent each of the features described in the claims of this disclosure. The teachings of *Wallach* seem unrelated to the claims when the claims are viewed as a whole. Thus, the Examiner is attempting to piece together the claimed invention using the claims as a guide. "It is impermissible to use the claimed invention as an instruction manual or "template" to piece together the teachings of the prior art so that the claimed invention is rendered obvious. . . . One cannot use hindsight reconstruction to pick and choose among isolated disclosures in the prior art to deprecate the claimed invention." *See In re* Fitch, 972 F.2d 1260, 23 USPQ2d 1780, 1784 (Fed. Cir. 1992).

Accordingly, the rejection of claims 3-7 under 35 U.S.C. § 103(a) should be overturned.

Issue 5: Whether claims 8, and 11-12 are unpatentable under 35 U.S.C. § 103(a) over *Salo, Susai, Rajakarunanayke,* and *Wallach* in further view of U.S. Patent No. 6,138,049 (*McLaughlin*).

By virtue of their dependence on claim 1, claims 8, and 11-12 incorporate the limitations of claim 1. For reasons previously discussed, these elements are not taught or suggested alone or in combination over *Salo. Susai,* and *Rajakarunanayke.* Further, the inclusion of *Wallach* is improper as discussed above. The use of a fifth reference *McLaughlin* to reject claims 8, and 1-12 further suggests that the Examiner is using improper hindsight. As with *Wallach*, the Examiner appears to be using hindsight reconstruction to pick and choose among isolated disclosures in the prior art to deprecate the claimed invention. In this case, the Examiner cites *McLaughlin* as allegedly teaching a method whereby designated telephony node determines which of the multiple servers is the designated server by communicating with the database, where the designated database telephony node is the notification client, and communicates with the database through the notification manager and vice verse." *See* Office Action Page 13-14.

The Examiner further asserts, with regard to claim 8, that it would have been obvious to one of ordinary skill in the art . . . to modify *Salo* so that the database communicated with the designated telephony node concerning the primary server so the system can immediately recover from a server failure without the need for a notification recovery request by the telephony node. Claim 8, however, has no such requirement related to server failures or recovery requests by any telephony node. Claim 8 requires that "the designated telephony node determines which of the multiple servers is the designated server by communicating with the database."

McLaughlin, is related to improved process control systems capable of generating and distributing notifications immediately upon recovery of a process controller, without the need for a notification recovery request by a notification client and to a system capable of distributing notifications rapidly from one network node to a plurality of notification clients. *See* col. 2, lines 56-64.

Considering the claims as a whole, the designated telephony node is designated such that the existing data channel can be identified. Distributing notification data and synchronizing notification clients as taught by *McLaughlin* does not teach or suggest claims 8, and 11-12 as a whole, which requires establishing a data tunnel through a firewall of the remote enterprise network and then using a telephony node to determine which of multiple servers is communicating over the existing channel with the network database.

Accordingly, the rejection of claims 8, and 11-12 under 35 U.S.C. § 103(a) should be overturned.

Issue 6: Whether claims 17, 18 and 25 are unpatentable under 35 U.S.C. § 103(a) over *Salo, Susai,* and *Rajakarunanayke* in further view of U.S. Patent No. 6,081,900 (*Subramaniam*).

By virtue of their dependence on claims 13 and 23, claims 17 and 18 incorporate the limitations of claim 13 and claim 25 incorporates the limitations of claim 23. *Subramaniam* is cited as teaching that reply data is received through port 443 and that the reply data is received using Secure Sockets Layer. When the claims are taken as a whole, however, *Subramaniam* fails to remedy the deficiencies of *Salo, Susai,* and *Rajakarunanayke* as previously discussed. For example, *Subramaniam* provides a distributed computing system which allows secure external access to a secure network. *Subramaniam* uses a border server inside the secure network to connect a client to a target server. *See* col. 3, lines 15-25. *Subramaniam* does not teach that the connection between the border server and the target server occurs through a firewall or that the connection is established and kept open in response to a request from the target server. More particularly, *Subramaniam* teaches URL transformations and HTTP redirection and SSL software to provide secure authentication of a user from an external client and to provide secure transmission of confidential data between the target server and the external client. *See* col. 3, line 66 – col. 4, line 5. URL transformations, HTTP redirection and SSL software to provide secure authentication does not suggest establishing a data channel through a firewall of an enterprise network that is kept open with ongoing reply data sent by a data center.

Accordingly, the rejection of claims 17, 18, and 25 under 35 U.S.C. § 103(a) should be overturned.

Issue 7: Whether claim 19 is unpatentable under 35 U.S.C. § 103(a) over *Salo, Susai,* and *Rajakarunanayke* in further view of U.S. Patent No. 6,295,551 (*Roberts*).

By virtue of its dependence on claim 13, claim 19 incorporates the elements of claim 13. For reasons previously discussed, these elements are not taught or suggested alone or in combination over *Salo, Susai,* and *Rajakarunanayke. Roberts* was cited by the Examiner as teaching that it is well known in the art for port 80 to be used for the server to communicate over the web. However, *Roberts* fails to teach or suggest, as required by claim 13:

> transmitting a data request to the remote data center;
>
> receiving reply data that has been transmitted by the remote data center in response to the data request and that establishes the data tunnel with the remote data center, the data tunnel operating as a virtual private network through a firewall of the enterprise network without requiring a virtual private network node to be placed at the firewall;
>
> receiving the reply data from the remote data center in an ongoing manner such that the data tunnel is kept open . . . .

Claim 13, which is from the perspective of the enterprise network, establishes the data tunnel with a remote data center through a firewall of the enterprise network. Claim 13 also requires that the data tunnel be kept open by receiving ongoing rely data from the remote data center. Claim 13 also requires that the data tunnel exist prior to receiving an access request for network data.

Roberts is directed to a call center system that allows a representative and a user to jointly brows WWW content while simultaneously conducting a voice conversation. One of skill in the art is unlikely to view incorporating call center systems that allow the joint browsing of WWW content (*See* abstract) as teaching the establishment of a data tunnel that is kept open between a data center and an enterprise network using ongoing reply data. These teachings of *Roberts* are also unlikely to be viewed as teaching situations where the data tunnel exists prior to receiving an access request to the network data.

As with previous applications, the citation of *Roberts* is an impermissible use the claimed invention as an instruction manual or "template" to piece together the teachings of the prior art so that the claimed invention is rendered obvious. As previously stated, "One cannot use hindsight reconstruction to pick and choose among isolated disclosures in the prior art to deprecate the claimed invention." *See In re* Fitch, 972 F.2d 1260, 23 USPQ2d 1780, 1784 (Fed. Cir. 1992).

The Examiner fails to consider the claim as a whole. Thus, in addition to being an improper combination, *Roberts* does not teach or suggest the deficiencies of *Salo, Susai,* and *Rajakarunanayke.*

Accordingly, the rejection of claim 19 under 35 U.S.C. § 103(a) should be overturned.

Issue 8: Whether claims 20 and 24 are unpatentable under 35 U.S.C. § 103(a) over *Salo, Susai,* and *Rajakarunanayke* in further view of U.S. Patent No. 6,631,416 (*Bendinelli*).

By virtue of their status as dependent claims, claim 20 incorporates the elements of independent claim 13, and claim 24 incorporates the elements of claim 23. For reasons previously discussed, these elements are not taught or suggested alone or in combination over *Salo, Susai,* and *Rajakarunanayke. Bendinelli* was cited by the Examiner as teaching encrypting the network data to comply with SSL and transmitting the network data to the remote data center through a second data channel such that the transmission of the network data operates as a temporary virtual private network. However, *Bendinelli* fails to teach or suggest the claims when viewed as a whole.

As previously stated, each of claims 20 and 24 requires a data tunnel established between a data center and an enterprise network. Claims 20 and 24 further require the data channel to be through a firewall of the enterprise network and that the data tunnel be established prior to an access request for network data. Further, claims 20 and 24 also require the data tunnel to be kept open using reply data sent in an ongoing manner to the enterprise network.

While the data tunnel of claims 20 and 24 is established between the data center and the enterprise network, *Bendinelli* teaches the establishment of a virtual private network between a first and second processor using an <u>additional</u> processor that may indicate consent on behalf of the first processor to enable a tunnel between the first and second processors. *See* col. 3 line 63 – col. 4 line 5. *Bendinelli* does not suggest that the tunnel be formed prior to receiving an access request nor does *Bendinelli* teach or suggest that the data tunnel is kept open via the transmission of ongoing reply data. Thus, the combination of *Salo, Susai, Rajakarunanayke* and *Bendinelli* fails to teach or suggest the claimed invention.

Accordingly, the rejection of claims 20 and 24 under 35 U.S.C. § 103(a) should be overturned.

Issue 9: Whether claim 36 is unpatentable under 35 U.S.C. § 103(a) over *Salo, Susai,* and *Rajakarunanayke* in further view of U.S. Patent No. 6,529,500 (*Pandharipande*).

By virtue of its dependence on claim 34, claim 36 incorporates the elements of claim 34. For reasons previously discussed, these elements are not taught or suggested alone or in combination over *Salo, Susai,* and *Rajakarunanayke. Pandharipande* is directed to methods and apparatus for unified messaging. *Pandharipande* teaches a messaging interface configured to provide an indication of a number of messages for each of a plurality of message types. *See* col. 2, lines 28-31. However, no discussion is present related to the establishment of a data tunnel between a data center and an enterprise network that is kept open by transmitting reply data in an ongoing matter. For at least these reasons and other discussed herein, the combination of *Salo, Susai, Rajakarunanayke* and *Pandharipande* fails to teach or suggest the claimed invention.

Accordingly, the rejection of claim 36 under 35 U.S.C. § 103(a) should be overturned.

Conclusions

Based on the foregoing, Appellant respectfully requests that the Board reverse the Examiner's rejections of Claims 1-45 pending in this application, which would then place this application in condition for immediate allowance.

Dated this 13th day of January, 2006.

Respectfully submitted,

Carl T Reed

CARL T. REED
Attorney for Appellant
Registration No. 45,454

WORKMAN NYDEGGER
1000 Eagle Gate Tower
60 East South Temple
Salt Lake City, Utah 84111
Telephone: (801) 533-9800
Fax: (801) 328-1707

C:\DOCS\15964\5.1\DFW0000013143V001.DOC

IX. CLAIMS APPENDIX

1. (Previously Presented) In a data center capable of communicating with a remote enterprise network, a method for enabling a user to access network data of the remote enterprise network through a data tunnel between the data center and the remote enterprise network that operates as a virtual private network, the method comprising the acts of:

in response to receiving a data request from the remote enterprise network, establishing the data tunnel with the remote enterprise network by transmitting reply data to the remote enterprise network, the data tunnel operating as a virtual private network through a firewall of the remote enterprise network without requiring a virtual private network node to be placed at the firewall;

continuing to transmit the reply data to the remote enterprise network in an ongoing manner such that the data tunnel is kept open;

receiving an access request from a user for network data from the remote enterprise network;

transmitting the access request to the remote enterprise network using the existing data tunnel that has been established and exists prior to the data center having received the access request;

receiving the network data from the remote enterprise network in response to the access request; and

transmitting the network data to the user.

2. (Previously Presented) A method as defined in claim 1, wherein the access request is received by a designated server, and wherein the designated server is one of multiple servers of the data center.

3. (Previously Presented) A method as defined in claim 2, wherein a database of the remote enterprise network is notified which of the multiple servers is the designated server, the designated server notifying the database when the data tunnel is established.

4. (Original) A method as defined in claim 3, wherein the access request is received by a designated telephony node of the data center, and wherein the user generates the access request using a telephone system.

5. (Original) A method as defined in claim 3, wherein the access request is received by one of multiple servers of the data center over the Internet, and wherein the access request is generated by the user using a device connected to the Internet.

6. (Original) A method as defined in claim 4, wherein the designated telephony node of the data center transmits the access request to the designated server.

7. (Original) A method as defined in claim 6, wherein the designated telephony node determines which of the multiple servers is the designated server by communicating with at least one of the multiple servers.

8. (Original) A method as defined in claim 6, wherein the designated telephony node determines which of the multiple servers is the designated server by communicating with the database.

9. (Original) A method as defined in claim 1, wherein the act of receiving an access request to access network data of the remote enterprise network from the user further comprises the act of authenticating the identity of the user.

10. (Original) A method as defined in claim 9, wherein authenticating the identity of the user comprises the act of receiving a valid personal identification number.

11. (Original) A method as defined in claim 4, wherein the act of transmitting the network data to the user includes the acts of:

transmitting the network data from the designated server to the designated telephony node; and

transmitting the network data from the designated telephony node to the telephone system used by the user.

12. (Original) A method as defined in claim 5, wherein the act of transmitting the network data to the user includes the act of transmitting the network data from the designated server to the device that is connected to the Internet.

13. (Previously Presented) In an enterprise network capable of communicating with a remote data center network, a method for enabling a user to access network data of the enterprise network through a data tunnel between the remote data center and the enterprise network that operates as a virtual private network, the method comprising the acts of

transmitting a data request to the remote data center;

receiving reply data that has been transmitted by the remote data center in response to the data request and that establishes the data tunnel with the remote data center, the data tunnel operating as a virtual private network through a firewall of the enterprise network without requiring a virtual private network node to be placed at the firewall;

receiving the reply data from the remote data center in an ongoing manner such that the data tunnel is kept open;

receiving, from the remote data center, an access request to access network data of the enterprise network, the access request having been received by the remote data center from the user and thereafter transmitted by the remote data center to the enterprise network through the data tunnel that has been established and exists prior to the remote data center having received the access request; and

in response to the access request, transmitting the network data to the remote data center such that the user is enabled to access the network data.

14. (Original) A method as defined in claim 13, wherein the data request includes a uniform resource identifier.

15. (Previously Presented) A method as defined in claim 13, wherein the data request is transmitted through the firewall.

16. (Original) A method as defined in claim 15, wherein the data request is transmitted through a proxy server.

17. (Original) A method as defined in claim 13, wherein the reply data is received through port 443.

18. (Original) A method as defined in claim 17, wherein the reply data is received using Secure Sockets Layer protocol.

19. (Original) A method as defined in claim 13, wherein the reply data is received through port 80.

20. (Original) A method as defined in claim 13, wherein the act of transmitting the network data to the remote data center includes the acts of:

encrypting the network data to comply with Secure Sockets Layer protocol,

transmitting the network data to the remote data center through a second data tunnel, such that the transmission of the network data operates as a temporary virtual private network; and

closing the second data tunnel.

21. (Original) A method as defined in claim 13, wherein upon receiving the access request, the method further comprises the act of:

performing an act upon the network data.

22. (Original) A method as defined in claim 21, wherein performing an act upon the network data includes retrieving email message data.

23. (Previously Presented) In a data center capable of communicating with a remote enterprise network, a method for enabling a user to access network data of the remote enterprise network through a data tunnel between the data center and the remote enterprise network that operates as a virtual private network, the method comprising the acts of:

receiving, from the remote enterprise network, a uniform resource identifier associated with a resource of a server of the data center;

in response to receiving the uniform resource identifier, invoking the resource to establish the data tunnel with the remote enterprise network by transmitting reply data, and continuing to transmit the reply data to the remote enterprise network in an ongoing manner, such that the data tunnel is kept open between the data center and the remote enterprise network, the data tunnel operating as a virtual private network through a firewall of the remote enterprise network without requiring a virtual private network node to be placed at the firewall;

receiving an access request to access network data of the remote enterprise network from the user;

inserting the access request into the reply data and transmitting the access request to the remote enterprise network using the data tunnel that has been established and exists prior to the data center having received the access request;

receiving the network data from the remote enterprise network in response to the access request; and

transmitting the network data to the user.

24. (Original) A method as defined in claim 23, wherein the act of receiving the network data from the remote enterprise network comprises the act of receiving through a second data tunnel the network data from the remote enterprise network, the second data tunnel operating as a temporary virtual private network is closed after the network data is received by the data center.

25. (Original) A method as defined in claim 23, wherein the act of transmitting the access request to the remote enterprise network comprises the act of transmitting the access request using Secure Sockets Layer protocol.

26. (Original) A method as defined in claim 23, wherein the act of receiving an access request to access network data of the remote enterprise network from the user further comprises the act of authenticating the identity of the user.

27. (Original) A method as defined in claim 26, wherein authenticating the identity of the user comprises the act of receiving a valid personal identification number.

28. (Currently Amended) A computer program product for implementing in a data center a method for enabling a user to access network data of a remote enterprise network through a data tunnel between the data center and the remote enterprise network that operates as a virtual private network, the computer program product comprising:

a computer-readable medium carrying computer-executable instructions for implementing the method, the computer-executable instructions comprising:

program code means for establishing the data tunnel with the remote enterprise network by transmitting reply data to the remote enterprise network in response to receiving a data request from the remote enterprise network, the data tunnel operating as a virtual private network through a firewall of the remote enterprise network without requiring a virtual private network node to be placed at the firewall;

program code means for continuing to transmit the reply data to the remote enterprise network in an ongoing manner such that the data tunnel is kept open;

program code means for receiving an access request from a user for network data from the remote enterprise network;

program code means for transmitting the access request to the remote enterprise network using the data tunnel that has been established and exists prior to the data center having received the access request;

program code means for receiving the network data from the remote enterprise network in response to the access request; and

program code means for transmitting the network data to the user.

29. (Original) A computer program product as defined in claim 28, wherein the computer-executable instructions further comprise program code means for authenticating the identity of the user.

30. (Original) A computer program product as defined in claim 28, wherein the computer-executable instructions further comprise program code means for enabling telephony nodes of the data center to receive the access request and to transmit the access request to a designated server, wherein the designated server is transmitting the ongoing reply data to the remote enterprise network.

31. (Original) A computer program product as defined in claim 30, wherein the designated server is one of multiple servers of the data center, and wherein the user generates the access request using a telephone system.

32. (Original) A computer program product as defined in claim 28, wherein the computer-executable instructions further comprise program code means for caching a copy of network data in a database of the data center.

33. (Original) A computer program product as defined in claim 32, wherein the computer-executable instructions further comprise program code means for transmitting the cached copy of the network data to the user in response to receiving the access request from the user.

34. (Previously Presented) In an enterprise network capable of communicating with a remote data center, a method for enabling a user to manipulate network data of the enterprise network through a data tunnel between the remote data center and the enterprise network that operates as a virtual private network, the method comprising the acts of

transmitting a data request to the remote data center;

receiving reply data that has been transmitted by the remote data center in response to the data request and that establishes the data tunnel with the remote data center, the data tunnel operating as a virtual private network through a firewall of the enterprise network without requiring a virtual private network node to be placed at the firewall;

receiving the reply data from the remote data center in an ongoing manner such that the data tunnel is kept open;

receiving, from the remote data center, a user request for an act to be performed on network data of the enterprise network, the user request having been received by the remote data center from the user and thereafter transmitted by the remote data center to the enterprise network through the data tunnel that has been established and exists prior to the data center having received the user request; and

upon receiving the user request, performing the act on network data of the enterprise network.

35. (Previously Presented) A method as defined in claim 34, wherein performing an act upon the network data includes deleting email.

36. (Previously Presented) A method as defined in claim 35, wherein performing an act upon the network data includes faxing the network data to the user.

37. (Previously Presented) A method as defined in claim 35, wherein performing an act upon the network data includes retrieving a web page.

38. (Previously Presented) A method as defined in claim 35, wherein performing an act upon the network data includes retrieving email messages.

39. (Previously Presented) In a data center capable of communicating with a remote enterprise network, a method for enabling a user to access network data of the remote enterprise network through a data tunnel between the data center and the remote enterprise network that operates as a virtual private network, the method comprising:

establishing the data tunnel with the remote enterprise network by transmitting reply data to the remote enterprise network in response to receiving a data request from the remote enterprise network;

continuing to transmit the reply data to the remote enterprise network in an ongoing manner to keep the data tunnel open;

receiving network data from the remote enterprise network through the data tunnel, the data tunnel operating as a virtual private network through a firewall of the enterprise network without requiring a virtual private network node to be placed at the firewall;

caching a copy of the network data in a database of the data center;

receiving an access request to access network data of the remote enterprise network from the user;

retrieving the network data from the database in response to the access request; and

transmitting the network data to the user.

40. (Original) A method as defined in claim 39, wherein the network data of the enterprise network is disconnected from the enterprise network after the network data is received by the data center.

41. (Original) A method as defined in claim 39, wherein the network data of the enterprise network is disconnected from the user after the network data is received by the data center.

42. (Original) A method as defined in claim 39, wherein the user determines what network data is transmitted to the data center, and wherein the user determines what network data is cached in the database.

43. (Original) A method as defined in claim 39, wherein the act of receiving an access request to access network data of the remote enterprise network from the user further comprises the act of authenticating the identity of the user.

44. (Original) A method as defined in claim 39, wherein the access request comprises a command to update network data.

45. (Previously Presented) A method as defined in claim 44, further comprising the acts of updating the cached copy of network data, and transmitting update information to the enterprise network.

Claims 46-48. (Canceled)

X. EVIDENCE APPENDIX

None.

XI. RELATED PROCEEDINGS APPENDIX

None.